

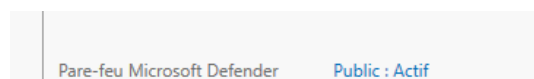
Mathéo

Intro :

Dans ce tp nous allons améliorer la sécurité de notre serveur AD ainsi que notre windows serveur et on finira avec l'installation de windows Laps. Ces mesures visent à améliorer la sécurité pour se défendre de potentielles attaques malveillantes.

Commençons avec le Durcissement et Sécurité Windows Server.

Rendons-nous sur l'ad et on va réactiver tous les pare-feu désactivés



Windows

(1) Pare-feu et protection du

Qui et ce qui peut accéder à vos réseaux.

Réseau avec domaine

Le pare-feu est activé.

Réseau privé

Le pare-feu est activé.

Réseau public (actif)

Le pare-feu est activé.

Puis il faut effectuer les mises à jour et cocher les cases suivantes

Options avan

***Votre organisation gère certain**

Options de mise à jour

Recevoir les mises à jour d'autre

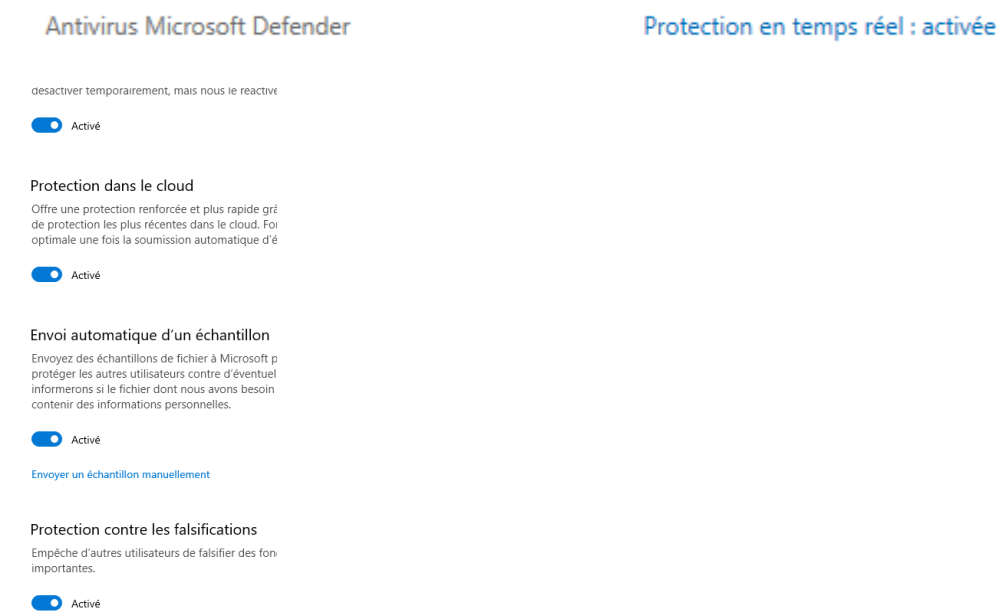
Activé

Téléchargez les mises à jour via c

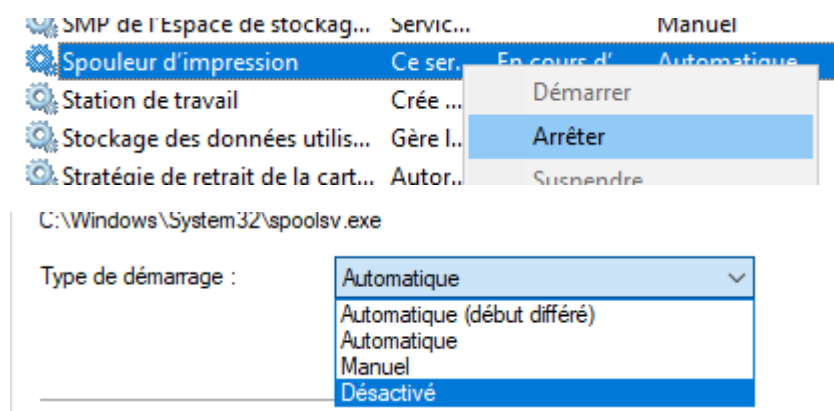
Désactivé

Redémarrez cet appareil dès que
l'appareil doit être allumé et bra

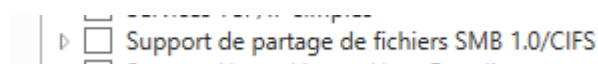
Et dans les paramètres de l'antivirus directement cocher toutes les cases de protection.



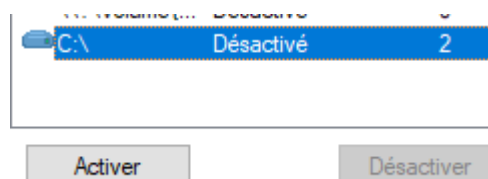
Ensuite comme notre serveur n'utilise pas d'imprimante on va désactiver et arrêter le spouleur d'impression dans les services.



Il faut vérifier aussi à bien désactiver la fonctionnalité smb 1.0 obsolète.



On va ensuite par sécurité activer les clichés instantanés sur notre disque C.



On peut également les planifier si besoin par jours

ect.

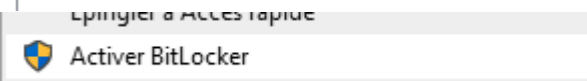
Volume	Heure de la procha...	Part
\\?\Volume{...}	Désactivé	0
C:\	10/12/2024 12:00	2

ement avec BitLocker dans les fonctionnalités.



Clichs instantanés du volume sélectionné

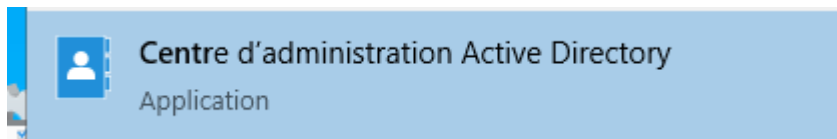
10/12/2024 09:56 r BitLocker sur le disque



Puis il faudra simplement choisir le répertoire où l'on enregistrera le fichier correspondant à la clé de récupération et enfin il faudra choisir le dernier type de chiffrement.

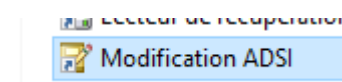
Deuxième partie pour notre tp on va passer à la Sécurité contrôleur de domaine Active Directory.

On va se rendre dans le centre d'administration.

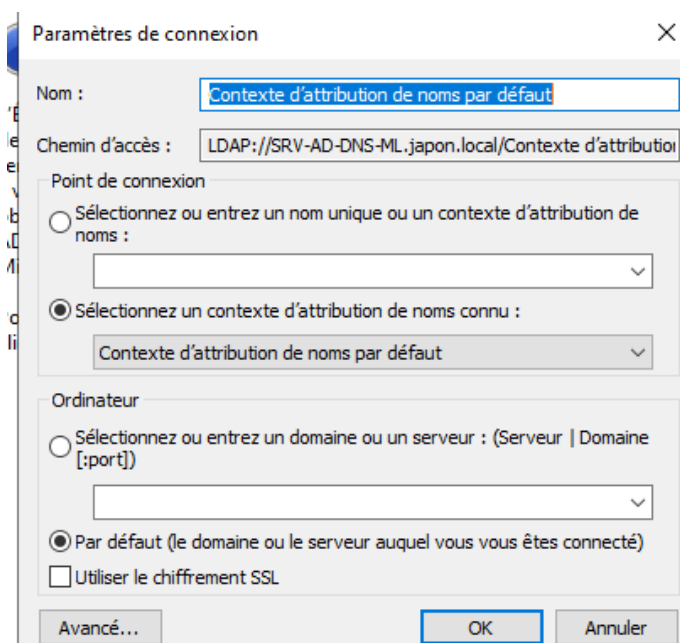


Et on active la corbeille ce qui nous permettra de rétablir les éventuelles suppressions accidentelles.

Ensuite on se rend dans l'outil d'administration suivant.

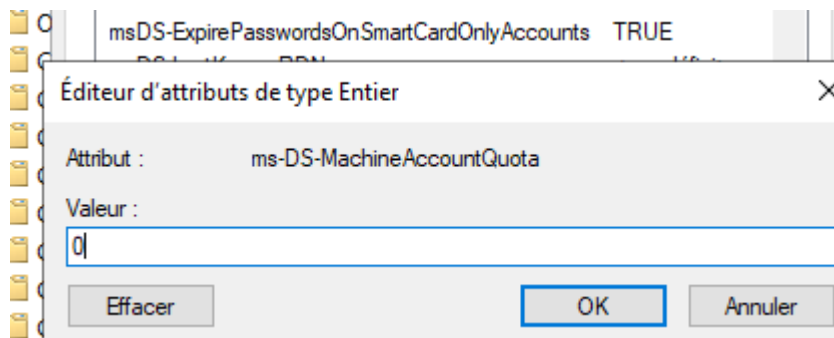


Puis sur action on fait connexion et la fenêtre suivante apparaît.



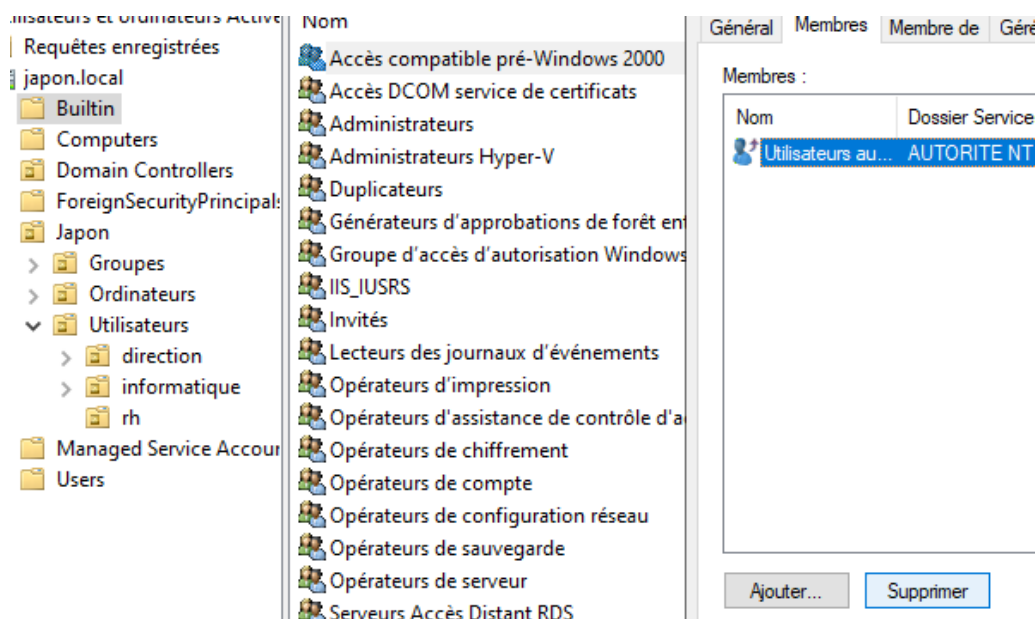
Et on fera juste OK sans rien toucher.

Puis dans les propriétés du domaine dans l'éditeur d'attribut on va chercher



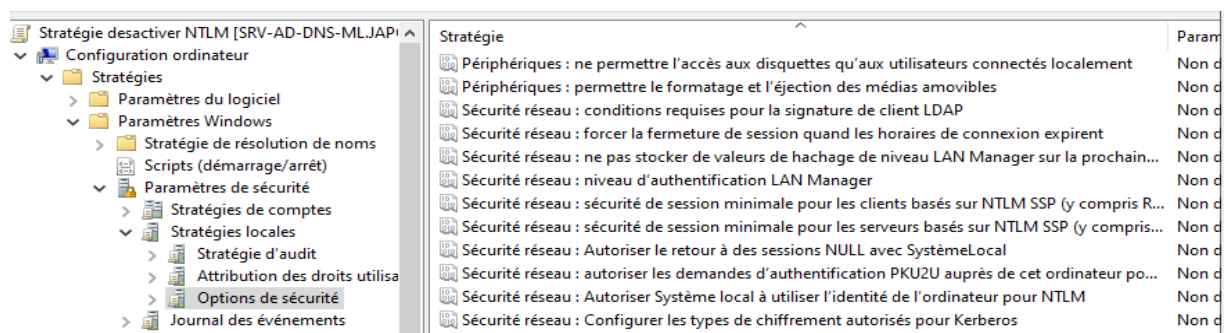
Et en double cliquant dessus on le mettra à 0. Ce paramètre à 0 fera qu'uniquement les admins pourront mettre des machines au domaine.

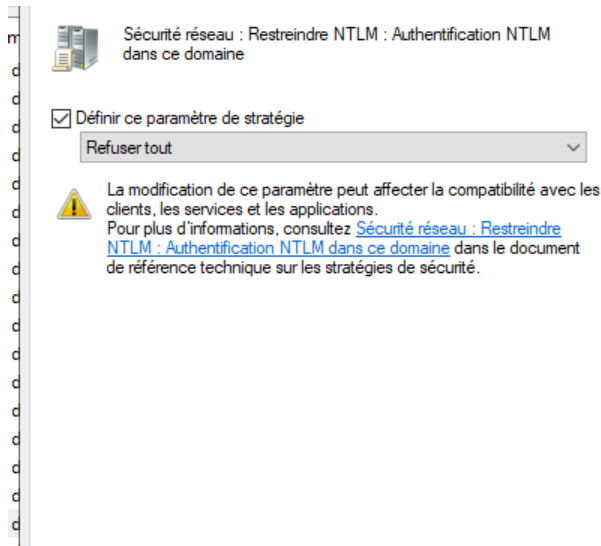
On va maintenant se rendre dans l'ad et supprimer les droits de rétrocompatibilité avant windows 2000



Ensuite dans le gestionnaire de stratégie de groupe.

On va Désactiver NTLMv1 et NTLMv2 qui sont des protocoles parfois utilisés mais dangereux.





Puis retournons sur l'ad et on va faire quelque manipulation pour veiller a la bonne sécurité de l'utilisateur kerberos qui sert a l'authentification.

Et on va lancer le powershell et faire quelques commandes.

```
PS C:\Users\Administrateur> cd c:\
```

```
PS C:\> cd .\ResetKRBTGT\
```

```
PS C:\ResetKRBTGT> powershell -executionpolicy bypass .\Reset-KrbTgt-Password-For-RWDCs-And-RODCs.ps1
```

powershell -executionpolicy bypass .\Reset-KrbTgt-Password-For-RWDCs-And-RODCs.ps1

Ensuite une nouvelle fenêtre s'ouvre.

Puis quelques étapes à suivre.

```
: Do you want to read information about the script, its functions, its behavior and the impact? [YES | NO]: no
```

```
[2024-12-10 11:42:25] : Please specify the mode of operation: 6
```

Juste entrée pour celui en dessous

```
For the AD forest to be targeted, please provide the FQDN or press [ENTER] for the current AD forest:  
:  
For the AD domain to be targeted, please provide the list nr or the FQDN or press [ENTER] for the current AD domain:  
:
```

De même.

Puis

```
Which KrbTgt account do you want to target?  
- 1 - Scope of KrbTgt in use by all RWDCs in the AD Domain  
- 0 - Exit Script  
Please specify the scope of KrbTgt Account to target: 1_   
[CONTINUE | STOP]: CONTINUE_
```

| pwdLastSet 10/12/2024 11:47:33 Paris, Madrid Le mot de passe à bien été changé on a maintenant terminé la sécurisation de l'ad et on va passer a la dernière partie avec l'installation de windows laps